PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-003224
(43)Date of publication of application : 08.01.1992

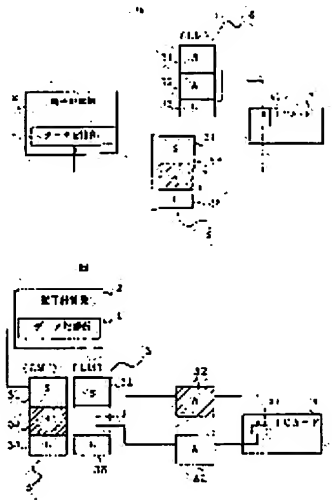
(51)Int.Cl. G06F 9/06
// G06K 17/00

(21)Application number : 02-104599
(22)Date of filing : 20.04.1990

(71)Applicant : N T T DATA TSUSHIN KK
(72)Inventor : TAKEUCHI TAKASHI
HIRANO KAZUYA
KOBAYASHI TAKAFUMI
RI EISEN

(54) METHOD FOR MANAGING SOFT MODULE BY IC CARD

(57)Abstract:
PURPOSE: To improve the safety with regard to an illegal copy, etc., by enciphering a soft module with the individual key of an IC card and a cipher generating means by using the IC card, and decoding the enciphered soft module with the individual key of the IC card used for the encipherement and a decoding generating means.
CONSTITUTION: When an origin load module 3 is stored in a data recording part 1 of an electronic computer 2, a controller of the origin load module 3 of a software, or a person having proprietary rights disturbs and enciphers a partial module 'A' 32 of the origin load module 3 by a ciphere function (F) and a secret individual key (K) incorporated in an IC part 41 of an IC card 4, and remakes it to an enciphered loading module 5. In order to actuate normally the enciphered load module 5, it is decoded by using the only IC card 4 having the same individual key as that of the time when a partial module 'A" 52 is generated. In such a manner, it is possible to cope with a misuse attending to an illegal copy and a theft, etc., of the soft module.



⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−3224

⑤1Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 9/06	450 B	7927−5B
// G 06 K 17/00	L	6711−5L

⑬公開　平成4年(1992)1月8日

審査請求　未請求　請求項の数 1　(全7頁)

⑤4発明の名称　ICカードによるソフトモジュールの管理方法

⑳特　願　平2−104599
㉒出　願　平2(1990)4月20日

⑦2発明者　竹内　隆　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑦2発明者　平野　一哉　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑦2発明者　小林　孝文　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑦2発明者　李　暎瑄　東京都港区虎ノ門1丁目26番5号　エヌ・テイ・テイ・データ通信株式会社内
⑦1出願人　エヌ・テイ・テイ・データ通信株式会社　東京都港区虎ノ門1丁目26番5号
⑦4代理人　弁理士　磯村　雅俊

明細書

1．発明の名称

ICカードによるソフトモジュールの管理方法

2．特許請求の範囲

(1)電子計算機の処理手順を記述したソフトモジュールであり、マイクロプロセッサを内蔵し、個別鍵と暗号作成手段および復号作成手段を有するICカードを用いて、上記ソフトモジュールの一部もしくは全部を、上記ICカードの個別鍵と暗号作成手段により暗号化し、該暗号化したソフトモジュールを起動する場合には、該暗号化したソフトモジュールの暗号化に用いたICカードの個別鍵と復号作成手段により、該暗号化したソフトモジュールの一部もしくは全部を復号化することを特徴とするICカードによるソフトモジュールの管理方法。

3．発明の詳細な説明

[産業上の利用分野]

本発明は、FD(Flexible Disk)や、端末の記憶装置などに格納されるソフトモジュールのセキュリティ管理方法に係り、特に、ICカードを用いて、ソフトモジュールの暗号化、および、復号化を行ない、ソフトモジュールの不正コピーなどの悪用を効率良く防止するのに好適なICカードによるソフトモジュールの管理方法に関するものである。

[従来の技術]

現在、コンピュータは、その処理速度、および、演算機能の高信頼性により、広い分野で利用されている。

コンピュータが正常に動作するためには、その動作順序や内容を書き示したプログラム、すなわち、ソフトモジュールが必要である。特に、近年は、コンピュータ分野において、このソフトモジュールの良否で、コンピュータシステムの善し悪しが決まるほどであり、コンピュータにおけるソフトモジュールの開発に、多くのコストをかけている。

しかし、このように大きなコストをかけて開発

したソフトモジュールは、コピーが容易であり、その保護が大きな問題となっている。

そのために、ソフトモジュールを知的所有権の保護の対象として、著作権を与え、その不正な使用を防止することなどが検討されている。

また、データの機密保護と合わせて、パスワードを設定して、パスワードを知っている正しい利用者以外に対しては、それ以上のソフトモジュールの動作を受け付けず、データの利用を許さないようにする方法がある。

パスワードより、さらに、データの機密保持に有効なものとして、データの暗号化がある。暗号の目的は、データの機密保持を行ない、不正使用を防止するものである。例えば、あるメッセージを、暗号化鍵を用いて暗号化し、正規のデータ利用者は、復号化鍵を用いて、この暗号化されたメッセージを復号して、正確なメッセージを得るようにしたものである。

このような、暗号化鍵、および、復号化鍵をＩＣカードに埋め込み、管理するものがある。例えば、ＩＤ(ＩDentifier)カードや、クレジットカードであり、これらに埋め込まれた暗号化鍵、および、復号化鍵により、情報の暗号化を行ない、個人の情報の保護を行なっている。

ＩＣカードは、広義には、集積回路を含むカード全てをさすが、特に、マイクロプロセッサとメモリを含むものは、通常の磁気カードと異なり、暗号化機能と復号化機能を有し、偽造や不正読み出しを防ぐためのセキュリティ機能を持たせることが出来る。

このような、暗号理論や、ＩＣカードに関しては、電子情報通信学会編「電子情報通信ハンドブック」(１９８８年、オーム社発行)のｐｐ.３５７～３６２、および、ｐｐ．６０３～６０４に記載されている。

〔発明が解決しようとする課題〕

このように、多額のコストがかかり、かつ、重要なデータが記録されているソフトモジュールの保護管理に関して、従来は、著作権による法的な保護や、パスワードによるソフトウェアによる保護管理方法があった。

しかし、著作権による保護では、実際に不正使用が発見されなければ、効果はなく、利権を有するものが、不正使用者による不正使用を探し出さなければならず、大きな負荷がかかっていた。また、パスワードによる保護では、不正利用者が、何度も、様々なパスワードを入力することにより、最終的に不正にアクセスすることが出来る可能性が高い。

このように、従来のＦＤや、端末装置に格納されているソフトモジュールは、不正コピーなどに関して、安全性に欠けるところがあった。

すなわち、ソフトモジュール側は、ソフトを起動出来る者を限定出来ないという弱点があり、ＦＤや端末装置にアクセスできるものであれば、誰でも、ロードモジュール（ソースプログラムから、端末装置で実行可能な形式に生成したソフトモジュールであり、端末装置は、このロードモジュールを主記憶装置に格納して実行する）をコピーし、起動することが容易であり、悪用される恐れがあった。

本発明の目的は、これら従来技術の課題を解決し、ＩＣカードを用いて、ソフトモジュールの暗号化、および、復号化を行ない、ソフトモジュールを正常に起動出来る者を、ＩＣカードを所持する者に限定し、ソフトモジュールの不正コピーや盗難などに伴う悪用に対処することを可能とするＩＣカードによるソフトモジュール管理方法を提供することである。

〔課題を解決するための手段〕

上記目的を達成するため、本発明のＩＣカードによるソフトモジュールの管理方法は、マイクロプロセッサを内蔵し、個別鍵と暗号作成部、および、復号作成部を有するＩＣカードを用いて、ソフトモジュールの一部、もしくは、全部を、ＩＣカードの個別鍵と暗号作成部により暗号化し、この暗号化したソフトモジュールを起動する場合には、この暗号化したソフトモジュールの暗号化に用いたＩＣカードの個別鍵と復号作成部により、暗号化したソフトモジュールの一部、もしくは、

全部を復号化することを特徴とする。

〔作用〕

本発明においては、ソフトモジュールの全部、もしくは、セキュリティ部となる一部を、ＩＣカードのＩＣ部に内蔵している暗号作成部により、撹乱して暗号化する。

そして、この暗号化したソフトモジュールを、端末装置の記憶部、あるいは、ＦＤなどの外部記憶媒体に格納する。

この暗号化したソフトモジュールを、端末装置で起動して使用する場合は、その暗号化した部分を、暗号化に用いたＩＣカードと同じ個別鍵を有するＩＣカードの復号作成部により復号化する。そして、暗号化した端末装置の記憶部内、あるいは、外部記憶媒体内のソフトモジュールを正常に起動する。

このようにして、機密性の高いソフトモジュールを起動出来る者を、ＩＣカードを所持する者に限定し、ソフトモジュールの不正コピーや、盗難などに伴う悪用に対処する。

〔実施例〕

以下、本発明の実施例を、図面により詳細に説明する。

第１図は、本発明を施した電子計算機システムの本発明に係る処理の一実施例の概要を示す説明図である。

任意のロードモジュールを格納するデータ記録部１を有し、このデータ記録部１に格納したロードモジュールに基づき、種々の情報の処理を行なう電子計算機２、電子計算機２のデータ記録部１に格納され、電子計算機２で実行される正当なプログラムが書かれている元ロードモジュール（図中ＬＭと記載）３、元ロードモジュール３の暗号化と復号化を行なうＩＣ部４１を内蔵するＩＣカード４、そして、ＩＣカード４により、元ロードモジュール３の一部を暗号化して作成した暗号化ロードモジュール(図中ＬＭ’と記載)５から構成されている。

尚、元ロードモジュール３は、部分モジュール「Ｓ」３１、部分モジュール「Ａ」３２、部分モジュール「Ｌ」３３の三つの部分から構成され、そして、暗号化ロードモジュール５は、元ロードモジュール３の部分モジュール「Ａ」３２を、ＩＣカード４を用いて暗号化した部分モジュール「Ａ’」５２と、部分モジュール「Ｓ」３１、および、部分モジュール「Ｌ」３３から構成されている。

本実施例においては、元ロードモジュール３の一部を、秘密の個別鍵を持つＩＣカード４で暗号化し、暗号化ロードモジュール５として電子計算機２のデータ記録部１に格納する。そして、起動時には、暗号化した暗号化ロードモジュール５を、暗号化に用いた同じ個別鍵を持つ唯一のＩＣカード４で復号化して、元ロードモジュール３に戻し、正常に起動させるまでの処理を示している。

第１図(ａ)は、元ロードモジュール３の暗号化に係る処理の概要を示す説明図である。

元ロードモジュール３は、ソースモジュールをコンパイルして、実行可能な状態にしたロードモジュールである。

この元ロードモジュール３を電子計算機２に保存しておく際に、データの暗号化と復号化が可能なＩＣカード４により、元ロードモジュール３の部分モジュール「Ａ」３２を暗号化する。

すなわち、ソフトの元ロードモジュール３の管理者、あるいは、所有権を有するものは、元ロードモジュール３を、電子計算機２のデータ記録部１に格納する時に、元ロードモジュール３の部分モジュール「Ａ」３２を、ＩＣカード４のＩＣ部４１に内蔵されている暗号関数(Ｆ)と、秘密の個別鍵(Ｋ)により、撹乱させて暗号化し、暗号化ロードモジュール５に作り換える。

第１図においては、元ロードモジュール３（ＬＭ）、暗号化ロードモジュール５（ＬＭ’）、および、秘密の個別鍵(Ｋ)の関係は、次の式により表される。

$$LM = S + A + L$$

とした場合、

$$LM' = S + F(A, K) + L$$

となる。

すなわち、部分モジュール「Ｓ」３１と、部分

モジュール「L」３３は変化せず、部分モジュール「A」３２のみが、ＩＣカード４のＩＣ部４１に内蔵されている暗号関数(F)と、秘密の個別鍵(K)により撹乱され、部分モジュール「A'」５２に暗号化される。

このように生成されたロードモジュールを、暗号化ロードモジュール５としている。

この暗号化ロードモジュール５を、電子計算機２のデータ記録部１に格納すれば、たとえ不正コピーされたり、盗まれたりしても、その暗号文を復号する個別鍵を有する唯一のＩＣカード４がない限り、正常には起動出来ない。

このようにして、ＩＣカード４を用いることにより、ソフトモジュールにセキュリティを持たせることが出来る。

次に、暗号化ロードモジュール５の復号化に関して説明する。

第１図(b)は、暗号化ロードモジュール５の復号化に係る処理の概要を示す説明図である。

暗号化された部分モジュール「A'」５２を含む暗号化ロードモジュール５は、そのままでは、正常に起動させることが出来ない。これを正常に起動させるためには、部分モジュール「A'」５２を生成した時と同じ個別鍵を持つ唯一のＩＣカード４を用いて復号化する。

すなわち、暗号化ロードモジュール５を起動して、処理が、部分モジュール「S」３１から、部分モジュール「A'」５２に移ったときに、部分モジュール「A'」５２をＩＣカード４に渡して、ＩＣカード４内のＩＣ部４１の復号関数(F^{-1})と秘密の個別鍵(K)を用いて復号化する。つまり、部分モジュール「A'」５２から、部分モジュール「A」３２へ復号化し、暗号化ロードモジュール５を元ロードモジュール３に戻す。

これを式で表すと、

$LM = S + F^{-1}(A', K) + L$

となる。

この処理が終了すると、次の処理、すなわち、部分モジュール「L」３３の処理へと進み、元ロードモジュール３として、正常に動作させる。

このようにして、起動時には、暗号化した暗号化ロードモジュール５を、暗号化に用いた同じ個別鍵を持つ唯一のＩＣカード４により、元ロードモジュール３に戻すことにより、ＩＣカード４を所有する正当な利用者は、元ロードモジュール３による処理を行なうことができる。

尚、第１図の実施例においては、ＩＣカード４のデータの暗号・復号化機能を用いて、元ロードモジュール３の一部を、ＩＣカード４により暗号化・復号化しているが、元ロードモジュール３の全てを暗号化・復号化しても良い。

また、ロードモジュールに限らず、全てのソフトモジュール、例えば、ソースモジュールや、オブジェクトモジュールなどに対しても、同様な暗号化と復号化を行なうことが可能である。

このように、本実施例によれば、暗号化したソフトモジュールを、ＦＤまたは、電子計算機などに格納しておき、その起動時には、ＦＤや、電子計算機と対をなす唯一のＩＣカードを用いて、そのソフトモジュールの暗号化された部分を復号化することにより、そのソフトモジュールを正常に起動させる。そして、ソフトモジュールを起動出来る者をＩＣカードを所持する者に限定し、不正コピーや盗難などに伴う悪用に対処することが出来る。

第２図は、第１図における電子計算機システムの本発明に係る暗号化の処理動作を示すフローチャートである。

例えば、機密化の必要なロードモジュールを電子計算機のハードディスク、もしくは、ＦＤに格納する際に、ＩＣカードを用いて、そのロードモジュールを暗号化して格納するものである。

まず、第１図における元ロードモジュール３を生成する(ステップ２０１)。この元ロードモジュール３にセキュリティを施すために、暗号化により、第１図の暗号化ロードモジュール５とする場合には(ステップ２０２)、まず、セキュリティを施す部分、すなわち、第１図における部分モジュール「A」３２を、第１図のＩＣカード４に送る(ステップ２０３)。

部分モジュール「A」３２を受け取った第１図のＩＣカード４は、ＩＣ部４１で暗号化を行なう(ステップ２０４)。

他の暗号化すべきセキュリティ部分があれば(ステップ２０５)、ステップ２０３に戻り、次のセキュリティ部分の暗号化を行なう（ステップ２０４）。一方、全てのセキュリティ部分に対する暗号化が終了すれば(ステップ２０５)、暗号化した第１図の暗号化ロードモジュール５を、第１図における電子計算機２のデータ記憶部１、例えば、ハードディスクに格納して(ステップ２０６)、処理を終了する。

このように、生成したロードモジュールを、ＩＣカードにより暗号化することにより、このロードモジュールを操作出来る者をＩＣカードの管理者に限定し、ソフトウェアに対するセキュリティ管理を行なうことが出来る。

尚、本実施例では、ロードモジュールの一部分を暗号化しているが、ロードモジュール全部を暗号化しても良い。

次に、暗号化したロードモジュールを起動する場合に関しての説明を行なう。

第３図は、第１図における電子計算機システムの本発明に係る復号化の処理動作を示すフローチャートである。

例えば、ハードディスク、もしくは、ＦＤに格納した暗号化ロードモジュールを、電子計算機で起動する際に、暗号化に使用したＩＣカードを用いて、その暗号化ロードモジュールを復号化して起動するものである。

まず、第１図における電子計算機２のデータ記憶部１に格納してある暗号化ロードモジュール５を読み込み(ステップ３０１)、実行する（ステップ３０２）。

実行中に(ステップ３０３)、実行部分が暗号化した部分、すなわち、第１図の部分モジュール「A'」５２になれば（ステップ３０４)、その部分モジュール「A'」５２を第１図のＩＣカード４に送り(ステップ３０５)、そのＩＣカード４のＩＣ部４１で復号化を行なう(ステップ３０６)。

このＩＣカードが正当なものであり、復号化が正常に行なわれれば(ステップ３０７)、ステップ３０２に戻り、次の処理を実行する。

第１図の暗号化ロードモジュール５の復号化、および、実行を、全て完了すれば（ステップ３０３)、処理を終了する。

尚、ステップ３０７において、使用するＩＣカードが第１図のＩＣカード４ではなく、不正なものであり、復号化が失敗すれば、エラー通知を行ない(ステップ３０８)、処理を終了する。

このように、暗号化されたロードモジュールの起動は、暗号化に用いた唯一のＩＣカードのみで可能であり、このＩＣカードを持たない不正な利用者は、ロードモジュールを実行することが出来ない。このことにより、ロードモジュールの不正使用を防止することが可能となる。

特に、一般に市販されているソフト、例えば、ワープロ用ソフトに代表されるＦＤ等の単位で販売されているソフト群を、このように暗号化しておくことにより、不正コピー等の悪用を、容易に防止することが出来る。

以上、第１図と第２図により説明したように、本実施例では、ＩＣカードを用いて、ソフトモジュールの保護を可能にする。

すなわち、ＦＤやハードディスクなどに格納され、保存されるソフトモジュールの全部、または、一部を、そのソフトの管理者が所持する唯一のＩＣカードで暗号化しておくことにより、保存してあるソフトモジュールが、たとえコピーされ、盗まれたとしても、管理用の唯一のＩＣカードがない限り、ソフトモジュールを起動することは出来ない。このように、ソフトモジュールを管理する唯一のＩＣカードを所持する者のみに、ソフトモジュールの起動が許され、使用権が与えられるため、ソフトモジュールの不正使用を防止することが出来る。

【発明の効果】

本発明によれば、ＩＣカードを用いて、ソフトモジュールの暗号化、および、復号化を行ない、ソフトモジュールを正常に起動出来る者をＩＣカ

ードを所持する者に限定し、ソフトモジュールの不正コピーや盗難などに伴う悪用に対処することが可能となり、極めて高いソフトモジュールの安全性を保証することが出来る。

4．図面の簡単な説明

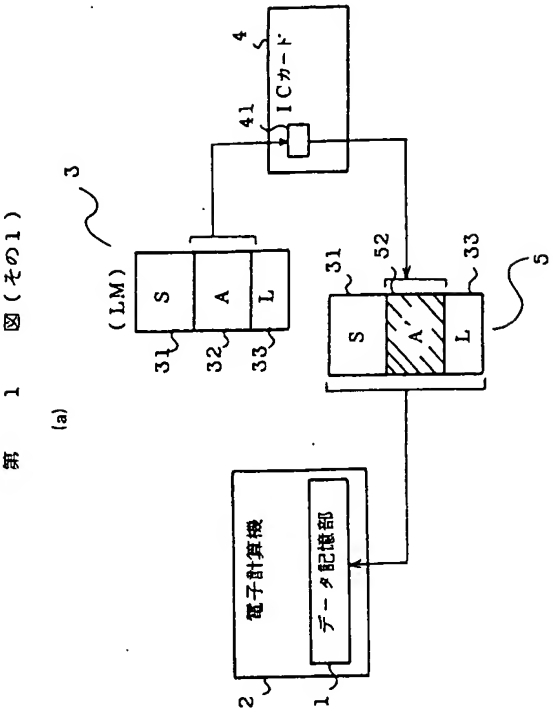
図面は本発明の実施例を示し、第1図は本発明を施した電子計算機システムの本発明に係る処理の一実施例の概要を示す説明図、第2図は第1図における電子計算機システムの本発明に係る暗号化の処理動作を示すフローチャート、第3図は第1図における電子計算機システムの本発明に係る復号化の処理動作を示すフローチャートである。

1：データ記録部，2：電子計算機，3：元ロードモジュール，4：ICカード，5：暗号化ロードモジュール，31：部分モジュール「S」，32：部分モジュール「A」，33：部分モジュール「L」，41：IC部，52：部分モジュール「A'」。

代理人 弁理士 鵜 村 雅 俊

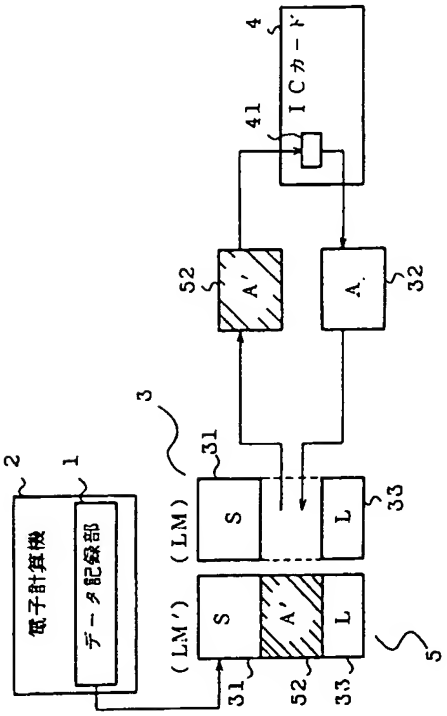
第 1 図（その1）

(a)

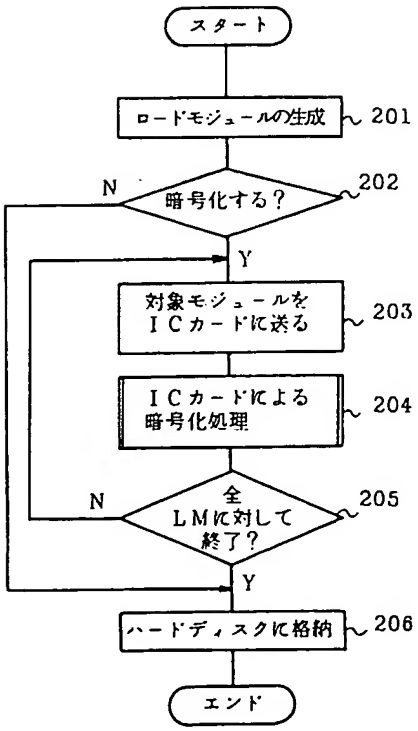


第 1 図（その2）

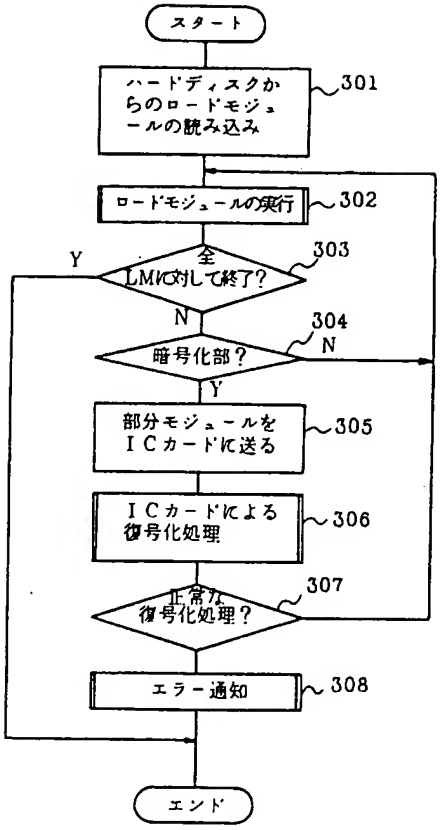
(b)



第 2 図



第　3　図


スタート
ハードディスクからのロードモジュールの読み込み
301
ロードモジュールの実行
302
全LMに対して終了?
303
Y
N
暗号化部?
304
N
Y
部分モジュールをICカードに送る
305
ICカードによる復号化処理
306
正常な復号化処理?
307
エラー通知
308
エンド